Los operadores detrás del troyano bancario Mekotio resurgieron con un cambio en su flujo de infección para permanecer fuera del radar y evadir el software de seguridad, mientras que organizaron casi 100 ataques en los últimos tres meses.

> *«Una de las principales características es el ataque modular que les da a los atacantes la capacidad de cambiar solo una pequeña parte del todo para evitar ser detectados»,* dijeron los investigadores de Check Point Research.

Se dice que la última ola de ataques apunta principalmente a víctimas ubicadas en Brasil, Chile, México, Perú y España.

El desarrollo se produce luego de que las fuerzas del orden españolas arrestaran en julio de 2021 a 16 personas pertenecientes a una red criminal en relación con la operación de Mekotio y otro malware bancario llamado Grandoreiro como parte de una campaña de ingeniería social dirigida a instituciones financieras en Europa.

La versión evolucionada de la cepa de malware Mekotio está diseñada para comprometer los sistemas Windows con una cadena de ataque que comienza con correos electrónicos de phishing disfrazados de recibos de impuestos pendientes y que contienen un enlace a un archivo ZIP o un archivo ZIP como archivo adjunto. Al hacer clic en abrir el archivo ZIP, se activa la ejecución de un script por lotes que, a su vez, ejecuta un script de PowerShell para descargar un archivo ZIP de segunda etapa.

Este archivo ZIP secundario alberga tres archivos diferentes: un intérprete de AutoHotkey (AHK), un script AHK y la carga útil DLL de Mekotio. El script de PowerShell antes mencionado luego llama al intérprete AHK para ejecutar el script AHK, que ejecuta la carga útil DLL para robar contraseñas de portales bancarios en línea y exfiltrar los resultados a un servidor remoto.

Los módulos maliciosos se caracterizan por el uso de técnicas simples de ofuscación, como cifrados de sustitución, que brindan al malware capacidades de sigilo mejoradas y permiten

que la mayoría de las soluciones antivirus no lo detecten.

> *«Existe un peligro muy real de que el banquero de Mekotio robe nombres de usuario y contraseñas para poder ingresar a las instituciones financieras. Por lo tanto, las detenciones detuvieron la actividad de las bandas españolas, pero no de los principales grupos de ciberdelincuencia detrás de Mekotio»,* dijo Kobi Eisenkraft.

Se recomienda encarecidamente a los usuarios de América Latina que utilicen la autenticación de dos factores para proteger sus cuentas de los ataques de adquisición y estén atentos a dominios similares, errores ortográficos en correos electrónicos o sitios web y mensajes de correo electrónico de remitentes desconocidos.